RECEIVED
CENTRAL FAX CENTER
APR 18 2005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Applicant: Dwork	)	Art Unit: 2135
Serial No.: 09/487,502	)	Examiner: Seal
Filed: January 19, 2000	)	AM9-99-0138
For: **DIGITAL SIGNATURE SYSTEM AND METHOD BASED ON HARD LATTICE PROBLEM**	)	April 18, 2005 750 B STREET, Suite 3120 San Diego, CA 92101

SUPPLEMENTAL APPEAL BRIEF

The appeal is reinstated. This supplemental brief is submitted in response to the attempt to reopen prosecution dated April 5, 2005. The relevant contents of the original brief are incorporated herein.

Table of Contents

(1) Real Party in Interest

See original brief.

(2) Related Appeals/Interferences

See original brief.

(3) Status of Claims

See original brief.

(4) Status of Amendments

See original brief.

(5) Summary of Invention

See original brief.

(6) Grounds for Rejection

(a) Claims 1, 2, 12, and 26 have been rejected under 35 U.S.C. §102 as being anticipated by Goldreich et al.

(b) Claims 3-11 and 13-25, and 27-35 have been rejected under 35 U.S.C. §103 as being unpatentable over Goldreich et al. in view of Diffie-Hellman.

(7a) Argument

The attempt to reopen prosecution is predicated on a false premise, namely, that Appellant requested reconsideration of the finality of the previous Office Action. Appellant did no such thing. Appellant appealed to the Board to obtain Board review, not to precipitate further churning of prosecution.

The attempt to reopen prosecution cited a new reference but failed to specify anything about the new reference other than the name. No PTO-892 accompanied the Office Action listing the new reference. Accordingly, Appellant had to telephone the Patent Office to discover what, precisely, was being cited against the claims. When contacted by phone the examiner asserted that the new reference was the one mentioned in the present background, but when the subsequently-faxed copy of the new reference was reviewed, it bore a different year of publication and different publication name than the reference cited in the background.

Appellant mentions these flaws not to quibble but to clarify that greater attention to detail is expected when, as here, the SPE has agreed to short-circuit the appellate process, cascade Appellant's costs, and draw

out prosecution time post-appeal.

In the substantive case, greater attention to detail could have spared this supplemental appeal brief. With more specificity, had the primary reference been closely reviewed, the allegation that it teaches using a function that renders infeasible the possibility of mapping two messages close together would never have been made. In the second paragraph of "our signature scheme" on page 3, the primary reference explicitly admits that in it, messages can be mapped close to each other, and that "messages close to each other will have the same signature". It further notes that sometimes this might be desired but in other cases, it is not. This is where the reference and the present claims diverge. Instead of recognizing that a mapping function can be used to render closeness infeasible, as set forth in, e.g., Claim 1, in those instances when it wishes to render closeness infeasible the reference first hashes the message, and only then maps it.

Indeed, the fact that the reference explicitly envisions that close mapping is sometimes desirable is a teaching away of a mapping function that always renders such infeasible, because if the reference were modified to have such a function, it would never achieve the close mapping that it asserts is "sometimes" desirable. Hence, the requirement in the reference to do something (such as a pre-map hash) outside of the mapping function in those instances wherein close mapping is not desired.

Appellant notes that on page 19, second paragraph, the reference explicitly teaches the above pre-map hash (that is, the hashed message is what is interpreted as a vector), but parenthetically notes that the hash alternatively can be used as "the means to map messages to such vectors". Apart from this curious and singular statement, however, the reference provides no clue as to how a hash function might be used to map something, as opposed to merely hashing. Does it replace the mapping function that is otherwise the subject of the reference? That would not make sense. To reconcile it with the rest of the teaching, the opaque

meaning of the statement might better be characterized as somewhat inaccurate shorthand jargon, the precise meaning of which is unclear. Accordingly, when read in context, it appears that the statement in the reference is of little use, failing, as it does, to explicate precisely what it is supposed to mean.

The rejections are even further afield with respect to independent Claim 12, which recites in part finding a point "y" of a key lattice $\mathcal{L}$ that is not the same as the auxiliary lattice on which the message point x is located, and independent Claim 26, which further specifies that the message μ or a concatenation thereof is mapped to a message point "x" in n-dimensional space, with the message point "x" being an element of a set of spaced-apart points that are not on the lattice. The first of these modalities for achieving the present advantages has been alleged to be taught in the primary reference, Sections 3.3 and 3.3.2, but this is simply not the case. The primary reference appears to use one and only one lattice. Specifically, the relied-upon portions teach first establishing a lattice dimension, and then using one of two distributions for the single lattice, namely, ***either*** random ***or*** rectangular. Not surprisingly, given that the primary reference does not appear to suggest two lattices in combination in the first place, the relied-upon sections fail to say anything about a point in one lattice (the auxiliary lattice, in Claim 12) being a map destination of a message and a point in another lattice ("key lattice") being used with the point in the first lattice, much less being used in combination with the other point as a digital signature.

The rejection alleges that section 5.1 of the primary reference teaches the limitation of Claim 26 of mapping the message to a message point "x" in n-dimensional space with the message point "x" being an element of a set of spaced-apart points not on the lattice. That does not appear to be the case. Nothing in Section 5.1 mentions non-lattice points, as best understood by Appellant. Certainly, the examiner has not tried to explain what, precisely, in Section 5.1 is a non-lattice point.

7(b)

Nowhere does the primary reference mention the equivalency of its pre-map hash to any other means for rendering infeasible mapping two messages close together, much less that it can be replaced by Diffie-Hellman, much less still how such a wholesale revision might be made or what likelihood of success it would have, see MPEP §2143. Likewise, the secondary reference discusses the Diffie-Hellman algorithm but not in the context of a replacement for anything, much less as a replacement in a lattice-based system. Diffie-Hellman does not even appear to recognize the concept of "lattice".

So what is the proferred Office Action rationale for combining? Because of the "brave new world" observation in Diffie-Hellman that "we are standing on the brink of revolution in cryptography". And thus the rejection descends into silliness. A general observation of incipient technological revolution cannot seriously be taken as a legitimate prior art suggestion to combine one specific thing with another specific thing when neither even mentions the other.

The rejections of certain dependent claims cannot be left unaddressed. It appears, for instance, that unnamed nineteenth century references not in evidence have been used in some opaque fashion to reject the limitation of Claims 4 and 28. Enough said. The collision intractability of the function in Claim 6 has been rejected based on the statement in Diffie-Hellman that "we are defining a function which is not invertible", in combination with the unsupported syllogistic minor premise that an invertible function is collision intractable (with the conclusion thus being that Diffie-Hellman teaches a collision intractable function). In patent law, an unsupported premise renders the syllogism false.

Continuing, Claim 7 requires that the collision intractability of the function "f" (rejected based on Diffie-Hellman, recall) is derived from the hardness of lattice problems (nowhere mentioned by Diffie-

Hellman), yet nonetheless Claim 7 has been rejected because the primary reference mentions lattices. The illogic here is easy to see. The relied-upon solution of Diffie-Hellman has nothing to do with lattices, and just because an unrelated reference mentions lattices does not motivate the skilled artisan to fit the square peg of Diffie-Hellman into the round hole of lattice problems, much less does it explain how, precisely, this might be approached.

Claim 8, requiring that the function "f" is not collision intractable, does not appear to have been considered.

Claim 11 requires that the predetermined distance is related to the number of dimensions in the lattice, and has been rejected based on Section 3.3.1 of the primary reference. Although credit is due for recognizing that Section 3.3.1 mentions the dimension of a lattice, that is all it does. Nowhere does it relate the dimension to a distance, much less the one claimed.

Respectfully submitted,

John L. Rogitz
Registration No. 33,549
Attorney of Record
750 B Street, Suite 3120
San Diego, CA 92101
Telephone: (619) 338-8075

JLR:jg

1053-73.APl

APPENDIX A - APPEALED CLAIMS

1. A computer-implemented method for digitally signing data, comprising:

generating a lattice $\mathcal{L}$ having at least one short basis establishing a private key and at least one long basis establishing a public key;

mapping at least the message μ or a concatenation thereof to a message point "x" in n-dimensional space using a function "f" rendering infeasible the possibility of mapping two messages together in the space; and

using the short basis, finding a lattice point "y" of the lattice $\mathcal{L}$ that is close to the message point "x".

2. The method of Claim 1, further comprising returning at least the message point "x" and the lattice point "y" as a digital signature.

3. The method of Claim 2, further comprising randomizing the function "f".

4. The method of Claim 3, wherein the function "f" is randomized by concatenating the message μ with a random number ρ.

5. The method of Claim 1, wherein the function "f" maps the message μ to a point on a grid.

6. The method of Claim 5, wherein the function "f" is collision intractable.

7. The method of Claim 6, wherein the collision intractability of the function "f" is derived from the hardness of lattice problems.

8. The method of Claim 5, wherein the function "f" is not collision intractable.

9. The method of Claim 1, wherein the function "f" maps at least the message to a point on an auxiliary lattice.

10. The method of Claim 1, further comprising verifying a digital signature at least in part by determining whether a difference between the lattice point "y" and the message point "x" is no more than a predetermined distance.

11. The method of Claim 10, wherein the predetermined distance is related to the number of dimensions in the lattice $\mathcal{L}$.

12. A computer program storage device including a program of instructions for generating a digital signature for a message, the program of instructions including:

computer readable code means for mapping a message μ or a concatenation thereof to a message point "x" in n-dimensional space, the message point "x" being a point of a grid or a point of an auxiliary lattice;

computer readable code means for finding a point "y" of a key lattice $\mathcal{L}$ that is not the same as the auxiliary lattice; and

computer readable code means for establishing a digital signature, based at least on the points "x" and "y".

13. The computer program storage device of Claim 12, wherein the means for mapping uses a function "f" rendering infeasible the possibility of mapping two messages close together in the space, and wherein the means for finding includes using a hard to find short basis of the key lattice $\mathcal{L}$.

14. The computer program storage device of Claim 13, further comprising means for randomizing the function "f".

15. The computer program storage device of Claim 14, wherein the function "f" is randomized by concatenating the message μ with a random number ρ.

16. The computer program storage device of Claim 12, wherein the function "f" maps the message μ to a point on a grid, and wherein the function "f" is collision intractable, the collision intractability being derived from the hardness of lattice problems.

17. The computer program storage device of Claim 12, wherein the function "f" is not collision intractable.

18. The computer program storage device of Claim 13, wherein the function "f" maps at least the message to a point on an auxiliary lattice.

19. A computer system for generating a digital signature of a message μ, comprising:

at least one sender computer including logic for executing method steps including:

mapping the message μ to a message point "x" at which it is not feasible to map any other message;

finding a lattice point "y"; and

transmitting at least the message μ and the points "x" and "y";

at least one receiver computer receiving the message μ and points "x" and "y" and including logic for executing method steps including:

determining whether a distance between the points "x" and "y" is related in a predetermined way to a predetermined distance, and based thereon determining whether the message μ has been properly signed.

20. The system of Claim 19, wherein the mapping act is undertaken using a function "f" that maps the message point "x" to a point of a grid or of an auxiliary lattice, and further wherein the lattice point "y" is a member of a lattice $\mathcal{L}$, and the finding act is undertaken using a hard-to-find short basis of the lattice $\mathcal{L}$.

21. The system of Claim 20, wherein the acts undertaken by the logic of the sender computer further comprise randomizing the function "f" by concatenating the message μ with a random number ρ.

22. The system of Claim 20, wherein the function "f" is collision intractable.

23. The system of Claim 22, wherein the collision intractability of the function "f" is derived from the hardness of lattice problems.

24. The system of Claim 20, wherein the function "f" is not collision intractable.

25. The system of Claim 20, wherein the predetermined distance is related to the number "r" of dimensions in the lattice $\mathcal{L}$.

26. A computer-implemented method for digitally signing data, comprising:
generating a lattice $\mathcal{L}$ having at least one short basis and at least one long basis;
mapping at least the message μ or a concatenation thereof to a message point "x" in n-dimensional space, the message point "x" being an element of a set of spaced-apart points not on the lattice; and
using the short basis, finding a lattice point "y" of the lattice $\mathcal{L}$.

27. The method of Claim 26, wherein the mapping is undertaken using a function "f".

28. The method of Claim 27, further comprising randomizing the function "f" by concatenating the message μ with a random number ρ.

29. The method of Claim 27, wherein the function "f" maps the message μ to a point on a grid.

30. The method of Claim 29, wherein the function "f" is collision intractable.

31. The method of Claim 30, wherein the collision intractability of the function "f" is derived from the hardness of lattice problems.

32. The method of Claim 29, wherein the function "f" is not collision intractable.

33. The method of Claim 27, wherein the function "f" maps at least the message to a point on an auxiliary lattice.

34. The method of Claim 26, further comprising verifying a digital signature at least in part by determining whether a difference between the lattice point "y" and the message point "x" is no more than a predetermined distance.

35. The method of Claim 34, wherein the predetermined distance is related to the number of dimensions in the lattice $\mathcal{L}$.